

MAY 08 2006**Yee &
Associates, P.C.**4100 Alpha Road
Suite 1100
Dallas, Texas 75244Main No. (972) 385-8777
Facsimile (972) 385-7766**Facsimile Cover Sheet**

To: Commissioner for Patents for Examiner Linh L. D. Son Group Art Unit 2135	Facsimile No.: 571/273-8300
From: Jane M. Roberts Legal Assistant to James O. Skarsten	No. of Pages Including Cover Sheet: 33
Message: Enclosed herewith: <ul style="list-style-type: none">• Transmittal Document; and• Supplemental Appeal Brief.	
Re: Application No. 09/810,288 Attorney Docket No: CA920000054US1	
Date: Monday, May 08, 2006	
Please contact us at (972) 385-8777 if you do not receive all pages indicated above or experience any difficulty in receiving this facsimile.	<i>This Facsimile is intended only for the use of the addressee and, if the addressee is a client or their agent, contains privileged and confidential information. If you are not the intended recipient of this facsimile, you have received this facsimile inadvertently and in error. Any review, dissemination, distribution, or copying is strictly prohibited. If you received this facsimile in error, please notify us by telephone and return the facsimile to us immediately.</i>

**PLEASE CONFIRM RECEIPT OF THIS TRANSMISSION BY
FAXING A CONFIRMATION TO 972-385-7766.**

RECEIVED
CENTRAL FAX CENTER

MAY 08 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Kou et al.

Serial No.: 09/810,288

Filed: March 16, 2001

For: Secure Session Management and
Authentication for Web Sites§
§
§
§
§
§

Group Art Unit: 2135

Examiner: Son, Linh L. D.

Attorney Docket No.: CA920000054US1

36736

PATENT TRADEMARK OFFICE
CUSTOMER NUMBERCertificate of Transmission Under 37 C.F.R. § 1.8(a)

I hereby certify this correspondence is being transmitted via
facsimile to the Commissioner for Patents, P.O. Box 1450,
Alexandria, VA 22313-1450, facsimile number (571) 273-8300
on May 8, 2006.

By:

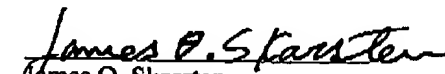

Jane M. RobertsTRANSMITTAL OF SUPPLEMENTAL APPEAL BRIEFCommissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450Sir:
ENCLOSED HEREWITH:

- Supplemental Appeal Brief (37 C.F.R. 41.37)

No fees are believed to be required. If, however, any fees are required, I authorize the
Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No 09-
0461.

No extension of time is believed to be necessary. If, however, an extension of time is required,
the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM
Corporation Deposit Account No 09-0461.

Respectfully submitted,



James O. Skarsten

Registration No. 28,346

Duke W. Yee

Registration No. 34,285

YEE & ASSOCIATES, P.C.

P.O. Box 802333

Dallas, Texas 75380

(972) 385-8777

ATTORNEYS FOR APPLICANTS

RECEIVED
CENTRAL FAX CENTER

MAY 08 2006

Docket No. CA920000054US1

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Kou et al.

Serial No. 09/810,288

Filed: March 16, 2001

For: Secure Session Management and
Authentication for Web Sites

Group Art Unit: 2135

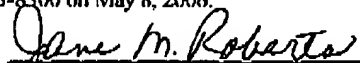
Examiner: Son, Linh L.D.

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Transmission Under 37 C.F.R. § 1.8(a)

I hereby certify this correspondence is being transmitted
via facsimile to the Commissioner for Patents, P.O. Box
1450, Alexandria, VA 22313-1450, facsimile number
(571) 273-8300 on May 8, 2006.

By:


Jane M. Roberts

SUPPLEMENTAL APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on March 6, 2006.

The fees required under § 41.20(B)(2), and any required petition for extension of time for filing this
brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF
SUPPLEMENTAL APPEAL BRIEF.

(Supplemental Appeal Brief Page 1 of 31)
Kou et al.— 09/810,288

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-34

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: 32 and 34
2. Claims withdrawn from consideration but not canceled: NONE
3. Claims pending: 1-31 and 33
4. Claims allowed: NONE
5. Claims rejected: 1-31 and 33
6. Claims objected to: NONE

C. CLAIMS ON APPEAL

The claims on appeal are: 1-31 and 33

STATUS OF AMENDMENTS

An amendment to the claims filed subsequent to the Final Rejection was not entered. Therefore, Claims 1-31 and 33 on appeal herein are as amended in the Response to Office Action filed October 14, 2004, and as set forth in the Appeal Brief filed August 23, 2005.

SUMMARY OF CLAIMED SUBJECT MATTER

A. CLAIM 1 - INDEPENDENT

The subject matter of Claim 1 is directed to a method of secure management and authentication between a web site and a web client, such as website 20 and web client 16 shown in Figure 1. The web site 20 has both secure web pages 32 and non-secure web pages 34, as shown by Figure 1 and taught at page 8, lines 6-9 of Applicants' specification. Steps of the method specify that a non-secure communication protocol and a session cookie are to be used, when a client requests access to non-secure web pages, and a secure communication protocol and an authcode cookie are to be used, when a client requests access to web pages. These steps of Claim 1 are supported by the application such as at page 5, lines 11-16. In addition, Claim 1 teaches that use of authcode cookies (for secure web pages) is interspersed between use of session cookies (for non-secure web pages). This Claim 1 feature is particularly supported at page 5, lines 20-22. Features of Claim 1 are additionally supported by steps 194 and 202-212 of Figure 6A.

B. CLAIM 12 - INDEPENDENT

The subject matter of Claim 12 is directed to a system for secure management and authentication between a web site and a web client. The system comprises a web server, having a web site and a web client coupled to the web server via a communication channel, wherein the web site includes secure and non-secure web pages. These elements of Claim 12 are supported in the application such as at Figure 1, which shows a communication channel 14 coupling a web server 12 to a web client 16, and a web site 20 of web server 12 includes secure web pages 32 and non-secure web pages 34. The above elements are further supported at page 6, line 24 through page 7, line 20 and page 8, lines 6-9 of Applicants' specification. Claim 12 further discloses that the web site includes a non-secure communication protocol and a session cookie that is used for allowing web client access to each one of the non-secure web pages and, a secure communication protocol and an authcode cookie that is used for allowing web client access only to the secure web pages. These features of Claim 12 are supported in the application such as at page 5, lines 11-22, and steps 152-174 of Figure 5B, together with the application at page 24, line 26 through page 25, line 15.

C. CLAIM 20 – INDEPENDENT

The subject matter of Claim 20 is directed to a computer program product in a computer readable medium for presenting content in a document. The claim is a computer program product counterpart claim to method Claim 1.

GROUND OF REJECTION TO BE REVIEWED ON APPEAL**A. GROUND OF REJECTION 1 (Claims 12-19)**

Claims 12-19 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,892,307 (Wood et al.).

B. GROUND OF REJECTION 2 (Claims 1-11 and 20-30)

Claims 1-11 and 20-30 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,892,307 (Wood et al.).

C. GROUND OF REJECTION 3 (Claims 31 and 33)

Claims 31 and 33 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,892,307 (Wood et al.) in view of U.S. Patent No. 6,092,196 (Reiche).

ARGUMENT

Recent Proceedings in Present Application

In a Final Office Action dated January 25, 2005, the Examiner rejected Claims 1-7, 10-17, 20-26, and 29-30 under 35 U.S.C. § 102(b), as being anticipated by U. S. Patent No. 5,966,705, to Koneru et al. Claims 8-9, 18-19, 27-28, 31 and 33 were rejected under 35 U.S.C. § 103(a), as being unpatentable over Koneru in view of U. S. Patent No. 6,092,196 to Reiche. In response to this Final Office Action, Applicants filed a Notice of Appeal on June 23, 2005, and filed a corresponding Appeal Brief on August 23, 2005.

On December 14, 2005, the Examiner mailed an Office Action (hereinafter "Current Office Action"), whereby prosecution in the above application was reopened. In the Current Office Action, Koneru et al. was apparently withdrawn as a reference against Applicants' claims.

However, the Current Office Action rejected Claims 1-30 under 35 U.S.C. § 103(a) as being obvious in view of U. S. Patent No. 6,892,307, to Wood et al. Claims 31 and 33 were rejected under 35 U.S.C. § 103(a) as being obvious in view of Wood et al. in combination with Reiche. In view of these rejections, Applicants hereby request reinstatement of the Appeal.

A. GROUND OF REJECTION 1 (Claims 12-19)

Claims 12-19 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,892,307 (Wood et al.).

A.1. Teachings and Purpose of Applicants' Claim 12

In making their invention, Applicants were concerned with communication between a web client and a web site having both secure and non-secure web pages. Applicants recognized that for web sites such as e-commerce web sites, it is necessary to allow for authentication and session management when holding a conversation with a web client. Session management enables a web site to remember a web client between different login sessions, whereas authentication is a security measure which assures a web site that a request came from the same web client who originally logged onto the web site.

As is well known to those of skill in the art, cookies are a popular method for session management between a web site and a web client. For non-secure web pages, communication protocol encrypts the data transmitted between the e-commerce web site and a web client.

Authentication and session management may be carried out by utilizing HTTP Basic Authentication, Name-Value Pair Authentication, or session cookies. However, for secure web pages, cookie based session management must incorporate a secure communication protocol, to prevent unauthorized users from stealing sensitive data contained in the cookie. One such protocol is HTTPS (HTTP/SSL), described hereinafter in further detail.

The above teachings of Applicants are set forth in the present application, such as at page 1, line 24-page 2, line 6, and page 3, lines 17-22 and page 5, lines 1-9 and page 5, lines 11-15, as follows:

To correct these problems, an e-commerce web site must allow for authentication and session management while holding a conversation with a web client. Further, a secure communication protocol must be used when sensitive information is transmitted between the web client and the e-commerce web site. Session management allows a web site to remember a web client between different login sessions whereas authentication is a security measure which assures a web site that a request came from the same web client who originally logged onto the web site. A secure communication protocol encrypts the data transmitted between the e-commerce web site and a web client. To accomplish authentication and session management, one may utilize HTTP Basic Authentication, Name-Value Pair Authentication or session cookies. [page 1, line 24-page 2, line 6]

Cookie based session management must incorporate a secure communication protocol to prevent unauthorized users from stealing sensitive data contained in the cookie. One such protocol is HTTPS (HTTP over SSL). The acronym SSL stands for Secure Socket Layer protocol which is an industry standard for transmitting information securely while using HTTP. HTTPS includes provisions for web server authentication (verifying the web server's identity to the web client), data encryption and web client authentication (verifying the web client's identity to the web server). [page 3, lines 17-22]

Furthermore, switching between HTTP and HTTPS can be troublesome because currently when a web client logs onto a web site using HTTPS, a cookie is issued to authenticate the web client, however, if the web client later browses a non-secure web page at the web site using HTTP, the same cookie is sent to the web client in clear text. At this point an unauthorized user can steal the cookie. Thus, using a single cookie under these circumstances jeopardizes the security of the web site.

Accordingly, there is a need for an improved secure session management and authentication method, using cookies, to protect both the web site and the web client from unauthorized users. The present invention addresses these needs. [page 5, lines 1-9]

The present invention provides a method for secure session management and authentication between a web site and a web client, the web site having secure and non-secure web pages, the method having the steps of utilizing a non-

secure communication protocol and a session cookie when the web client requests access to non-secure web pages; and utilizing a secure communication protocol and an authcode cookie when the web client requests access to secure web pages. [page 5, lines 11-15]

As indicated in the application at page 5, lines 1-6, Applicants recognized that there are significant problems in switching between a secure protocol such as HTTPS and a non-secure protocol such as HTTP, while using only a single type of cookie. For example, switching between HTTPS and HTTP can be troublesome in that when a web client logs on to a web site using HTTPS, a cookie is issued to authenticate the web client. If the web client later browses a non-secure page at the web site using HTTP, the same cookie is sent to the web client in clear text. At this point an unauthorized user can steal the cookie. Thus, using a single cookie in this situation, even if it is a secure cookie, can jeopardize the security of the web site. This is even more likely to happen when a user is continually switching between secure and non-secure web pages.

Applicants overcome the above drawbacks and disadvantages of the prior art by means of their invention, as set forth in Claim 12. Claim 12 provides that both different cookies and different protocols are to be used, depending on whether access is requested to secure or non-secure web sites. More particularly, Claim 12 recites that a secure cookie and protocol are to be used only to access secure web pages, whereas a non-secure cookie and protocol are to be used to access non-secure web pages. Claim 12 of Applicants' invention, in its present form, reads as follows:

12. A system, for secure session management and authentication between a web site and a web client, said system comprising a web server, a web client and a communication channel, said web server coupled to said web client via said communication channel, said web server having a web site, said web site including:
- a) secure and non-secure web pages;
 - b) a non-secure communication protocol and a session cookie for allowing said web client access to each one of said non-secure web pages; and
 - c) a secure communication protocol and an authcode cookie that is used for allowing said web client access only to said secure web pages.

A.2. Rejection of Claim 12 by Examiner

In the Office Action dated December 14, 2005, the Examiner stated the following:

17. As per claim 12:

Wood discloses "A system, for secure session management and authentication between a web site and a web client, said system comprising a web server, a web client and a communication channel, said web server coupled to said web client via said communication channel, said web server having a web site, said web site including:

a) secure (Col 7 lines 35-67) and non-secure web pages" in (Fig. 1, Col 5 lines 1-40, Col 8 lines 23-67);

The session cookie in Wood is the session cookie that has a low credential or trust level (Col 9 lines 20-25), and the authcode cookie is also the session cookie that has a high credential or trust level and the authentication information is encrypted (Col 8 line 65 to Col 9 line 25). Wood discloses in Col 8 lines 3-18 that the environmental information of the session (i.e. browser type, encryption capability, connection type and more) is used in some configurations for mapping particular authentication mechanisms to trust levels and for authorization decisions.

"b) a non-secure communication protocol and a session cookie that is used for allowing said web client access to each one of said non-secure web pages" in (Col 8 lines 44-55); and Wood further discloses of implementing multiple cookies or tokens to allow access different credential level or trust level resources (Col 8 lines 15-55) using the environmental information of the client session in (Col 19 line 42 to Col 20 line 40). "c) a secure communication protocol and an authcode cookie that is used for allowing said web client access only to said secure web pages" in (Col 7 line 35 to Col 8 line 10).

However, Wood does not directly disclose the "secure web pages".

Nevertheless, Wood does disclose of accessing secure resources using the browser and of implementing secure connection to the resource using encryption communication protocol, such as VPN, and SSL in (Col 7 lines 11-34, Col 7 line 58 to Col 8 line 22, and Col 18 lines 35-63).

Therefore, it would have been obvious at the time of the invention was made to one ordinary skill in the art to realize that the secure web pages are the secure resources accessing from the web browser through an encryption connection. [Office Action dated December 14, 2005, pp. 8-9]

In rejecting Claim 12, the Examiner cites sections of Wood that include, inter alia, excerpts thereof at col. 5, lines 1-40; col. 7, line 35-col. 8, line 10; col. 8, lines 15-55; col. 8, line 65-col. 9, line 25; col. 18, lines 35-63; and col. 19, line 42-col. 20, line 40. These excerpts of Wood, together with Figure 1 thereof, are as follows:

Session: A period and collection of states spanning one or more interactions between an entity and an information environment. As used herein a session may span multiple interactions with multiple resources of the information environment and, in some configurations, may span multiple information access protocols (e.g., HTTP, FTP, telnet, etc.). A session has a beginning and an end. During its existence, a session has state. As used herein, the term session connotes a greater persistence than as sometimes used to

describe the period of a "session layer" protocol interaction, which in the case of some protocols, such as HTTP, is generally very short-lived.

Single Sign-on Security Architecture

FIG. 1 provides an overview of major interactions between components for an exemplary security architecture in accordance with the present invention. As illustrated in FIG. 1, a client application, e.g., a browser 170 operated by a user, interacts with the security architecture via a gatekeeper and entry handler component 110 and a login component 120. Gatekeeper and entry handler component 110 provides an entry point for external client applications requesting access to enterprise applications and/or resources 190, including e.g., information resources 191, 192 . . . 193, for which access management is provided by the security architecture. Using facilities provided by a session management component 160, an authorization component 140, an authentication component 130, an identification component 150, and login component 120, the gatekeeper/entry handler component 110 allows, redirects or refuses access requests in accordance with a security policy.

Individual information resources typically have differing security requirements. In addition, individual types of access to a single information resource may have differing security requirements. Nonetheless, a given level of security may be sufficient for more than one of the information services or access types. For example, information resource 191 may include a product information service for providing general information such as product descriptions or data sheets to the public, while information resource 192 includes an order processing system for an eCommerce site. [Col. 5, lines 1-40]

Focusing then on an exemplary browser-type client entity, browser 170 requests access to one or more of enterprise applications and/or resources 190 (e.g., information resource 191) by presenting an URL to gatekeeper/entry handler component 110, which acts as a point of entry for client entities requesting access to applications and/or resources controlled by the security architecture. Gatekeeper/entry handler component 110 receives the request as a proxy for the requested resource. In some configurations, a combined gatekeeper/entry handler instance is provided, while in others, separate and/or multiple instances are provided with functionally identical interfaces to other components of the security architecture. In some configurations, multiple instances of entry handler functionality (e.g., interception of inbound requests and collection of environment information) are provided. For example, one or more instances for each of several connection types (e.g., dialup, WAN, etc.) may be employed. One or more instances of gatekeeper functionality (e.g., allowing access for authorized requests and otherwise denying or initiating appropriate responsive action) may also be provided. Configurations and functional decompositions suitable to a particular environment and expected load requirements will be appreciated by persons of ordinary skill in the art.

Entry handler functionality (e.g., in gatekeeper/entry handler component 110) ascertains much of the requesting client's environment information. For example, for dial up connections, environment information such as line speed and low-level line encryption are ascertained. Additional information, such as source number (e.g., from caller id information or based on a callback configuration), signaling type (e.g., POTS or digital ISDN), etc., may also be obtained. For network connections, similar environment information (e.g., source network and/or node, Virtual Private Network (VPN) low-level encryption, etc.) may be obtained from incoming requests themselves or based on a particular entry point (e.g., a particular router or port). More generally, gatekeeper/entry handler component 110 obtains and/or maintains information such as connect location (if

ascertainable), temporal information such as request time/date, session start time/date, etc. (preferably in both the client entity's frame of reference and the security architecture or requested information resource's frame of reference[**col. 7, line 35-col. 8, line 10**]

Such information is used in some configurations for mapping particular authentication mechanisms to trust levels and for authorization decisions. Environment information is generally packaged into a data structure that is associated with a client session. Other components of the security architecture may add additional client environment information, such as authentication strength or current trust level.

Gatekeeper functionality (e.g., in gatekeeper/entry handler component 110) checks whether a session is already associated with the incoming request. Although other techniques are possible, in some configurations in accordance with the present invention, gatekeeper/entry handler component 110 checks for the presence of a session token in the incoming request. Use of session tokens is described in greater detail below; however, in short, a session token may be any data supplied to the client entity for use in uniquely identifying an associated session. In general, preferred session token implementations are cryptographically secured and include facilities, such as expiration or mapping to a particular connection, to limit risk of replay attack and/or spoofing. Some session token implementations may encode session, principal, and/or trust level information. Some session token implementations may employ cookies, URL encoding, or other similar techniques for binding to incoming requests.

In some configurations, session tokens are employed to facilitate session continuity and to allow the security architecture to associate prior authentication of login credentials with an incoming access request. In one utilization, session tokens are issued to client entities as part of an interaction with the security architecture and are thereafter presented with access requests. In some configurations, new session tokens (each corresponding to a single session) are issued to client entity on each credential level change. In other configurations, a session token may remain the same even as credential levels are changed. Session continuity means the maintenance of coherent session state across one or more interactions between an entity and an information environment.[**col. 8, lines 15-55**]

For example, a principal id and current trust level are encoded in one realization of a cryptographically secured session credential and associated session token or cookie. In general, a variety of facilities, such as cookies, can be used to maintain state across a series of protocol interactions, such as HTTP transactions, that do not otherwise support persistent session state.

Referring again to FIG. 1, if a session token is present in the incoming request, gatekeeper/entry handler component 110 resolves the token to a session object. Alternatively, if no session token is present or if a session token is invalid, gatekeeper/entry handler component 110 establishes a new session (2). In an exemplary configuration in accordance with FIG. 1, session management component 160 allocates a new session and supplies associated default session credentials (2) based on the requested information resource and environment information. Note that a session is created irrespective of authentication status or identity, although some implementations may refuse to even allocate a session based on particular information resource requests and/or environment information. Given a session object, which may be resolved from a received session token or newly allocated, gatekeeper/entry handler component 110 interacts (3, 4) with authorization component 140 to determine whether the requested access is authorized. For some requested accesses and security policies (e.g., anonymous ftp access to certain archives), even a session without authenticated login credentials (trust level=0)

may be authorized. For others, a more substantial trust level may be required. [col. 8, line 65-col. 9, line 25]

As described above, login credentials (e.g., represented in a form such as exemplary login credentials structure 410) are obtained for a client entity. Typically, login credentials encoded in login credentials structure 410 are obtained from a principal via browser client and serve as evidence that the principal (e.g., a human user) is entitled to a particular identity. Accordingly, login credentials structure 410 encodes a `userId` and a `domainId` within which the `userId` should uniquely correspond to a principal. Specific login credentials, e.g., a password, a certificate, results of a biometric process, a response to an Enigma challenge or results of a smart card interrogation, etc. are encoded in login credentials structure 410, as a tagged value. An authenticationScheme is specified and creation time may be encoded to limit replay attacks. In the implementation of FIG. 4, login credentials structure 410 is encrypted using the public key of an authentication service (e.g., of authentication component 130). Because the key is public, any component, even untrusted components may encrypt login credentials for provision to authentication component 130, while only authentication component can decrypt the encrypted login credentials using its private key. In some configurations, secure transfer protocols, e.g., SSL, are employed to secure login credentials between a client entity such as browser 170 and the security architecture while encryption with a public key of an authentication service is performed within the security architecture, e.g., at login component 120. In other configurations, encryption with a public key of an authentication service may be performed at the client entity. [col. 18, lines 35-63]

Referring again to session credentials structure 420, a session id, a principal id, a trust level, group ids, a creation time and an expiration time are encoded in both in encrypted portion 421 and clear text portion 422. The session id is a unique identifier for a persistent session maintained by the security architecture. In implementations in which credential upgrade is provided or in which a session credential expiration and refresh is provided, multiple successively issued session credential instances may encode the same session id and correspond to the same persistent session. Principal id encodes an identifier for a principal to which the security architecture has resolved login credentials. For example, a login credential including a username `jdoe` and a password corresponding to `jdoe` may be resolved by the security architecture to a unique principal id associated with John. Q. Doe of the shipping and receiving department, having an employee badge number of 12345, etc.

In some embodiments, a trust level encodes the authorization level to which a principal has been authenticated. In such embodiments, the encoded trust level serves as a basis for evaluating whether a principal associated with the session credentials has been authenticated to a sufficient level for access to a requested resource. For example, a trust level of 5 may be sufficient for access to information resources having a trust level requirement of 5 or less. Trust levels offer an attractive decoupling of authorization levels and authentication methods as described elsewhere herein. However, in some embodiments, an authorization encoding may establish that a principal has been authenticated using a particular authentication mechanism. In either case, an authorization (e.g., encoded as a trust level) in a cryptographically secured session credential allows the security architecture to authorize accesses based on prior authentication of a login credential and without involvement of the authentication service.

Group ids can be used to grant or limit authorization scope based on group membership. Typically, session credentials serve as evidence of prior authentication and authorization for multiple accesses to information resources controlled by the security

architecture. However, session credentials may be replaced on a login credential upgrade as described elsewhere herein. In addition, session credentials of limited temporal validity may be refreshed by periodic replacement. In the configuration of session credentials structure 420, creation time and expiration time allow the security architecture to improve resistance to replay attacks. Session credentials typically have a relatively short expiration time (e.g., 15 minutes from creation or less) and underlying login credentials will be reauthenticated prior to expiration of the session credential. Assuming that the underlying login credentials, which are stored under the public key of authentication component 130, remain valid, authentication component 130 will issue a replacement cryptographically secured session credential (e.g., as session credentials structure 420). Depending on then current trust level mappings and, in some configurations, depending on then current environment parameters, the authorization accorded by the security architecture and encoded as a trust level may differ from that encoded in the session credential replaced. If a principal id or login credential has been revoked, reauthentication may fail and a user may be prompted to supply a sufficient login credentials as described elsewhere herein. Session id and principal id will typically remain the same for successive session credentials associated with a single persistent session. [col. 19, line 42-col. 20, line 40]

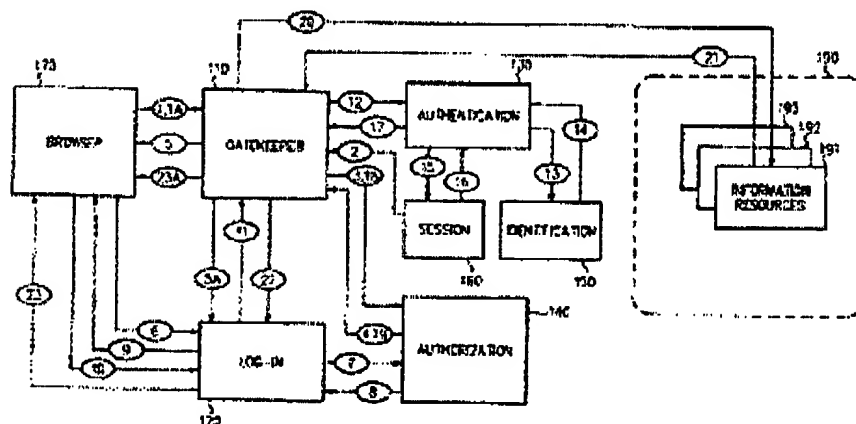


FIG. 1

A.3. Claim 12 Distinguishes over Wood et al. Reference

It is a fundamental principle of patent law that prior art must be considered in its entirety, MPEP 2141.02. Accordingly, the Abstract of the Wood reference, which contains very pertinent teachings, is set forth as follows:

Abstract

A security architecture has been developed in which a single sign-on is provided for multiple information resources. Rather than specifying a single authentication scheme for all information resources, the security architecture associates trust-level requirements with information resources. Authentication schemes (e.g., those based on passwords,

certificates, biometric techniques, smart cards, etc.) are associated with trust levels and a log-on service obtains credentials for an entity commensurate with the trust level requirement(s) of an information resource (or information resources) to be accessed. Once credentials have been obtained for an entity and the entity has been authenticated to a given trust level, access is granted, without the need for further credentials and authentication, to information resources for which the authenticated trust level is sufficient. (Emphasis added)

Thus, the Abstract of Wood states explicitly that once a credential has been obtained for an entity, and the entity has been authenticated to a given trust level, the entity needs no further credentials to access any information for which the given trust level is sufficient. Therefore, a principal teaching of Wood is that a single credential can be used to access information at different levels. This includes not only access to the highest level of authentication, that is, the “given” level, but also includes access to levels below the highest level, even to levels that are significantly below the highest level of authentication. This is obvious from the Wood Abstract, since a credential authenticated to a given trust level would clearly be sufficient for any level that was lower than the given trust level.

Applicants consider that the above principal teaching, set forth in the Wood Abstract, is in direct opposition to essential features of Applicants’ Claim 12. To the extent that there is any equivalency between Applicants’ Claim 12 and the Wood teaching, the given trust level of Wood would correspond to the secure web pages of Claim 12, and a trust level below the given level in Wood would correspond to the non-secure web pages of Claim 12. However, rather than the single credential of Wood, that can be used to access both trust levels, Claim 12 recites two different cookies. These are a session cookie and non-secure protocol for accessing non-secure web pages, and an authcode cookie and secure protocol for accessing secure web pages. Moreover, Claim 12 requires that the secure authcode cookie and protocol are to be used only to allow access to the secure web pages. Thus, Applicants’ Claim 12 prohibits use of the secure authcode cookie to access any web pages that are at a lower security or trust level, thus contradicting the principal teaching of Wood discussed above.

The above principal teaching of Wood, namely, that a single credential can be used to access information of different security levels, is emphasized repeatedly throughout the Wood disclosure. For example, such teaching is clearly stated in sections of Wood that were cited against Claim 12 in the Office Action. For example, Wood teaches at col. 5, lines 30-35, included in the cited section col. 5, lines 1-40, that “a given level of security may be

sufficient for more than one of the information services or access types”, even though both the information services and access types are taught to typically “have differing security requirements.” (Emphasis added).

Similarly, Wood at col. 19, lines 64-66, included in the cited section col. 19, line 42-col. 20, line 40, states that “a trust level of 5 may be sufficient for access to information having a trust level requirement of 5 or less.” (Emphasis added). This section of Wood clearly teaches away from the Claim 12 recitation that an authcode cookie, intended to allow access at the highest of two security levels, can be used to allow access only to such highest level. Applicants consider that other sections of Wood cited against Claim 12 either reinforce the above principal teaching of Wood, or contain unrelated teachings.

Applicants’ Claim 12 is considered to distinguish over Wood, particularly by reciting the above feature of a secure communication protocol and authcode cookie that is used for allowing web client access only to the secure web pages. However, in the Office Action, the only section of Wood cited against this essential feature of Claim 12 is the section at col. 7, line 35-col. 8, line 10. While this section appears to discuss client requests and associated environment information, it fails to provide any teaching in regard to security levels. Accordingly, this section of Wood does not disclose the above essential features of Claim 12.

In order for Claim 12 to be obvious in view of Wood, as contended in the Office Action, Wood would have to be modified in accordance with the teachings of Claim 1. However, it is well established that if the proposed modification of the prior art would change the principle of operation of the prior art being modified, then the teachings of the reference are not sufficient to render the claims *prima facie* obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959). **MPEP2143.02** Modifying Wood as taught by Applicants’ Claim 12 would, for example, limit the credential taught at col. 19, lines 60-66 to accessing information resources of trust level 5 only. Then, such credential could not be used to access information resources of less than trust level 5. In view of this substantial modification of an important principal of operation of Wood, it is abundantly clear that Applicants’ Claim 12 is not obvious in view of the Wood reference.

A fundamental principle taught by Applicants’ Claim 12 is the use of different cookies to access web pages of correspondingly different security levels. However, the Wood reference, such as at col. 1, lines 60-62, states that “individualized solutions make it difficult to maintain a uniform security policy across a set of applications or resources.” Thus, Wood not only fails to

disclose, suggest or provide motivation for the recitation of Applicants' Claim 1. In addition, Wood expressly teaches those of skill in the art reasons to not follow the above fundamental principle of Claim 1.

A.4. Conclusion

For at least all of the above reasons, Applicants respectfully submit that Wood et al. does not teach or suggest all of the features of Claim 12.

At least by virtue of their dependency on Claim 12, Wood et al. does not teach or suggest the features of dependent Claims 13-19.

Accordingly, it is respectfully requested that the Board reverse the Examiner's rejection of Applicants' Claims 12-19.

B. GROUND OF REJECTION 2 (Claims 1-11, 20-31 and 33)

Claims 1-11 and 20-30 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U. S. Patent No. 6,892,307 (Wood et al.).

B.1. Rejection of Claim 1 by Examiner

Applicants' Claim 1 currently reads as follows:

1. A method of secure session management and authentication between a web site and a web client, said web site having secure and non-secure web pages, said method comprising the steps of:
 - a) utilizing a non-secure communication protocol and a session cookie when said web client requests access to said non-secure web pages;
 - b) utilizing a secure communication protocol and creating an authcode cookie when said web client requests access to said secure web pages, so that utilizations of said authcode cookie are interspersed between utilizations of said session cookie, and at least some utilizations of said session cookie take place after utilizations of said authcode cookie.

In the Office Action dated December 14, 2005, the Examiner stated the following in regard to Claim 1:

7. As per claims 1:

Wood discloses "A method of secure session management and authentication between a web site and a web client, said web site having secure and non-secure web

(Supplemental Appeal Brief Page 19 of 31)
Kou et al., 09/810,288

pages, said method comprising the steps of: utilizing a non-secure communication protocol and a session cookie when said web client requests access to said non-secure web pages" in (Fig. 1, Col 5 lines 1-40, Col 8 lines 23-67);

The session cookie in Wood is the session cookie that has a low credential or trust level (Col 9 lines 20-25), and the authcode cookie is also the session cookie that has a high credential or trust level and the authentication information is encrypted (Col 8 line 65 to Col 9 line 25). Wood discloses in Col 8 lines 3-18 that the environmental information of the session (i.e. browser type, encryption capability, connection type and more) is used in some configurations for mapping particular authentication mechanisms to trust levels and for authorization decisions.

As evidence above, Wood teaches "utilizing a secure communication protocol and creating an authcode cookie when said web client requests access to said secure web pages". The secure communication protocol is the encrypted communication session environment in Col 8 lines 3-18.

Wood also further discloses "so that utilizations of said authcode cookie are interspersed between utilizations of said session cookie, and at least some utilizations of said session cookie take place after utilizations of said authcode cookie" in (Col 10 line 58 to Col 11 line 13, Col 13 lines 1-19, and Col 15 lines 1-57). Implementing multiple cookies or tokens allow access different credential level or trust level resources (Col 8 lines 1-55) with respect to the environmental information of the client session, such as a secure connection or VPN or Unsecure, in (Col 19 line 42 to Col 20 line 40).

However, Wood does not directly disclose the "secure web pages".

Nevertheless, Wood does disclose of accessing secure resources using the browser and implementing secure connection to the resource using encryption communication protocol, such as VPN, and SSL in (Col 7 lines 11-34, Col 7 line 58 to Col 8 line 22, and Col 18 lines 35-63).

Therefore, it would have been obvious at the time of the invention was made to one ordinary skill in the art to realize that the secure web pages are the secure resources accessing from the web browser through an encryption connection. [Office Action dated December 14, 2005, pp. 3-4]

Sections of Wood cited against Claim 1 at col. 10, line 58-col. 11, line 13, col. 13, lines 1-19 and col. 15, lines 1-57 are respectively set forth as follows:

Browser 170 sends (6) login component 120 a new access request using the URL specified in the redirect from gatekeeper/entry handler component 110. In configurations employing cookies as a medium for passing session tokens, the new access request will include the cookie and therefore the session token. Note that in configurations in which the security architecture controls access to resources in several domains, care should be exercised to select a tag or tags for the cookie such that it will be provided through normal operation of the browser in subsequent accesses to any of the several domains. Persons of ordinary skill in the art will appreciate suitable tagging techniques, including the use of multiple cookies. Login component 120 receives the access request and determines an appropriate authentication scheme based on mapping rules that identify those authentication schemes which are sufficient to achieve a given trust level. Preferably, the mapping rules are a function of environment information. In some configurations, mapping rules are implemented as fuzzy sets wherein acceptable authentication schemes are a function of required trust level and environment information.

In this way, environment affects the set of authentication schemes sufficient to meet a trust level requirement. [col. 10, line 58-col. 11, line 13]

In some embodiments in accordance with the present invention, session continuity is facilitated by supplying a session token to browser 170. For example in one configuration, login component 120 supplies a session token using a set cookie directive encoded with the results streamed (23) back to browser 170. In response, browser 170 stores the cookie using a tag (typically a filename encoding). Browser 170 supplies the cookie (and the session token) with subsequent access requests based on a correspondence between the tag and the requested resource. Typically, the correspondence is based on the second-level domain (e.g., sun.com) in which the requested resource is hosted, although nth-level domains or other resource identification and session token associating schemes may be employed. In configurations in which the security architecture controls access to multiple domains across which a spanning single sign-on is desired, multiple cookies may be employed. [col. 13, lines 1-19]

cryptographically secured session token or otherwise, session credentials may or may not be sufficient for access to the currently requested resource. For example, after a first access, the identity of an entity accessing resources controlled by the security architecture will be authenticated to a trust level sufficient for that access. Depending on the trust level requirements of a subsequent access and, in some configurations, depending on then current trust level mapping rules and environment information, the level of trust associated with a current session (e.g., as evidenced by current session credentials) may or may not be sufficient for the subsequent access. In situations for which a current level of trust (e.g., resulting from prior authentication of login credentials for an entity associated with the session) is sufficient for later access to the same or to another information resource, access is allowed without additional authentication. For example, in some security architectures in accordance with the present invention, the security architecture proxies (204) the request to the requested information resource and streams (205) a resulting response back to the requesting client entity. [col. 15, lines 1-57]

B.2. Claim 1 Distinguishes over Wood et al. Reference

Applicants' Claim 1 is considered to distinguish over the Wood et al. reference, particularly in reciting, in the over-all combination of Claim 1, utilizations of the authcode cookie that are interspersed between utilizations of the session cookie. Each of the sections of Wood cited against Claim 1 and set forth above are directed against this feature of Claim 1. However, while the above sections make reference to cookies, none of these sections appears to show or discuss an arrangement of cookies representing different security levels. Clearly, none of these sections shows or suggests utilizations of a cookie enabling secure access that are interspersed between utilizations of a cookie for lower or non-secure access, as recited by Applicants' Claim 1.

Moreover, Wood at col. 15, lines 6-16 expressly teaches away from such recitation of Claim 1. Specifically, such excerpt of Wood states that a credential used for a current session will also be used for later access, if the credential is sufficient for such later access. Thus, even

if the later access requires a lower security level than the current session, Wood teaches that the sufficient credential will be used, and not a lower level credential, as taught by Applicants' Claim 1.

Claim 20 is directed to subject matter similar to that of Claim 1, and is considered to distinguish over Wood et al. for the same reasons given in support thereof.

B.3. Conclusion

For at least all of the above reasons, Applicants respectfully submit that Wood et al. does not teach or suggest all of the features of Claims 1 and 20.

At least by virtue of their dependency on Claims 1 and 20, respectively, Wood et al. does not teach or suggest the features of dependent Claims 2-11 and 21-30.

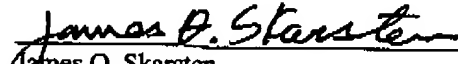
Accordingly, it is respectfully requested that the Board reverse the Examiner's rejection of Claims 1-11 and 20-30.

C. GROUND OF REJECTION 3 (Claims 31 and 33)

Claims 31 and 33 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,892,307 (Wood et al.) in view of U.S. Patent No. 6,092,196 (Reiche).

These claims respectively depend from and further restrict independent Claim 20. The Reiche patent does not supply the deficiencies in Wood et al. with respect to the independent claim, as discussed in detail above. Accordingly, for at least the reasons discussed above, Claims 31 and 33 are not obvious in view of any combination of Wood et al. and Reiche, and should be allowable in their present form.

Therefore, Claims 31 and 33 are believed to patentably distinguish over Wood et al. and Reiche, and any combination thereof, and it is respectfully requested that the Board reverse the Examiner's rejection of these claims.


James O. Skarsten
Reg. No. 28,346
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777

(Supplemental Appeal Brief Page 22 of 31)
Kou et al. - 09/810,288

CLAIMS APPENDIX

The text of the claims involved in the appeal are:

1. A method of secure session management and authentication between a web site and a web client, said web site having secure and non-secure web pages, said method comprising the steps of:
 - a) utilizing a non-secure communication protocol and a session cookie when said web client requests access to said non-secure web pages;
 - b) utilizing a secure communication protocol and creating an authcode cookie when said web client requests access to said secure web pages, so that utilizations of said authcode cookie are interspersed between utilizations of said session cookie, and at least some utilizations of said session cookie take place after utilizations of said authcode cookie.
2. The method of claim 1, wherein said method also comprises the steps of:
 - c) requesting said session cookie from said web client whenever said web client requests access to said non-secure web pages and verifying said requested session cookie; and
 - d) requesting said authcode cookie from said web client whenever said web client requests access to said secure web pages and verifying said requested authcode cookie.
3. The method of claim 2, wherein said method comprises repeatedly alternating between said secure communication protocol and said non-secure communication protocol when said web client alternates requests for access to said secure web pages and said non-secure web pages, respectively, and also repeatedly alternating between said utilizations of said authcode and said utilizations of said session code.

4. The method of claim 3, wherein said alternating between said secure communication protocol and said non-secure communication protocol is facilitated by a table which keeps track of said non-secure web pages and said secure web pages.
5. The method of claim 4, wherein said web site uses said table to direct said web client to use said secure communication protocol or said non-secure communication protocol depending on whether said web client requests access to said non-secure web pages or said secure web pages.
6. The method of claim 6, wherein said method also comprises allowing said web client to be a guest client or a registered client.
7. The method of claim 6, wherein said method also comprises creating stored information including data contained in said session cookie, data contained in said authcode cookie and data about said web client.
8. The method of claim 7, wherein said session cookie includes a pointer and an encrypted portion, said pointer pointing to said stored information, said encrypted portion having a random portion and a date portion.
9. The method of claim 7, wherein said authcode cookie includes an encrypted portion, said encrypted portion having a random portion and a date portion.
10. The method of claim 8, wherein verifying said requested session cookie from said web client includes using said stored information to generate a second session cookie and comparing

said second session cookie to said session cookie requested from said web client.

11. The method of claim 9, wherein verifying said requested authcode cookie from said web client includes using said stored information to generate a second authcode cookie and comparing said second authcode cookie to said authcode cookie requested from said web client.

12. A system, for secure session management and authentication between a web site and a web client, said system comprising a web server, a web client and a communication channel, said web server coupled to said web client via said communication channel, said web server having a web site, said web site including:

a) secure and non-secure web pages;

b) a non-secure communication protocol and a session cookie that is used for allowing said web client access to each one of said non-secure web pages; and

c) a secure communication protocol and an authcode cookie that is used for allowing said web client access only to said secure web pages.

13. The system of claim 12, wherein said web site also includes:

d) verification means for verifying said session cookie when said session cookie is requested from said web client; and

e) verification means for verifying said authcode cookie when said authcode cookie is requested from said web client.

14. The system of claim 13, wherein said web server further comprises a security alternating means for alternating between said secure communication protocol and said non-secure communication protocol.

15. The system of claim 14, wherein said web server further comprises a table to keep track of said non-secure web pages and said secure web pages.
16. The system of claim 13, wherein said web site includes access means to allow said web client to access said web site as a guest client or a registered client.
17. The system of claim 16, wherein said web system has storage means for containing stored information about said web client, data contained in said session cookie and data contained in said authcode cookie.
18. The system of claim 17, wherein said session cookie includes a pointer and an encrypted portion, said pointer pointing to said stored information, said encrypted portion having a random portion and a date portion.
19. The system of claim 17, wherein said authcode cookie includes an encrypted portion, said encrypted portion having a random portion and a date portion.
20. A computer program embodied on a computer readable medium, said computer program providing for secure session management and authentication between a web site and a web client, said web site having secure and non-secure web pages, said computer program adapted to:
- a) use a non-secure communication protocol and a session cookie when said web client requests access to said non-secure web pages;
 - b) use a secure communication protocol and an authcode cookie whenever said web client requests access to said secure web pages.

21. The computer program of claim 20, wherein said computer program is further adapted to:
- c) request said session cookie from said web client when said web client requests access to said non-secure web pages and to verify said requested session cookie; and
 - d) request said authcode cookie from said web client when said web client requests access to said secure web pages and to verify said requested authcode cookie.
22. The computer program of claim 21, wherein said computer program is further adapted to alternate between said secure communication protocol and said non-secure communication protocol when said web client alternates requests for access to said secure web pages and said non-secure web pages.
23. The computer program of claim 22, wherein said alternating between said secure communication protocol and said non-secure communication protocol is facilitated by a table which keeps track of said non-secure web pages and said secure web pages.
24. The computer program of claim 23, wherein said computer program uses said table to direct said web client to use said secure communication protocol or said non-secure communication protocol depending on whether said web client requests access to said non-secure web pages or said secure web pages.
25. The computer program of claim 22, wherein said computer program is adapted to allow said web client to be a guest client or a registered client.

26. The computer program of claim 25, wherein said computer program is adapted to create stored information including data contained in said session cookie, data contained in said authcode cookie and data about said web client.
27. The computer program of claim 26, wherein said session cookie includes a pointer and an encrypted portion, said pointer pointing to said stored information, said encrypted portion having a random portion and a date portion.
28. The computer program of claim 26, wherein said authcode cookie includes an encrypted portion, said encrypted portion having a random portion and a date portion.
29. The computer program of claim 27, wherein verifying said requested session cookie from said web client includes using said stored information to generate a second session cookie and comparing said second session cookie to said session cookie requested from said web client.
30. The computer program of claim 28, wherein verifying said requested authcode cookie from said web client includes using said stored information to generate a second authcode cookie and comparing said second authcode cookie to said authcode cookie requested from said web client.
31. The computer program of Claim 20, wherein said computer program is adapted to create a NAME attribute in a session cookie:
- a) generating a user_id;
 - b) generating a session_string;
 - c) generating a session_timestamp;

d) appending said session_timestamp to said session_string to create an intermediate value;

e) applying a one way hash function to said intermediate value to create a final value;
and

f) storing said final value in said NAME attribute.

33. The computer program of Claim 20, wherein said computer program is adapted to create a NAME attribute in an authcode cookie by:

a) generating an authcode;

b) generating an authcode_timestamp;

c) appending said authcode_timestamp to said authcode to create an intermediate value;

d) applying a one way hash function to said intermediate value to create a final value;

and

e) storing said final value in said NAME attribute.

EVIDENCE APPENDIX

There is no evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.